REMARKS

Reconsideration of this application, as amended, is respectfully requested. An RCE accompanies this amendment.

Claims 1-4 and 6-37 have been rejected.

In this response, claims 1, 8, 21, and 37 have been amended. Claim 7 has been canceled. No claims have been added. Support for the amendments is found in the specification, the drawings, and in the claims as originally filed. Applicants submit that the amendments do not add new matter.

Applicants reserve all rights with respect to the applicability of the Doctrine of Equivalents.

The Examiner objected to the specification stating that "the term 'computer readable storage medium"...is not defined in the specification."(Office Action, p. 3).

Applicants respectfully disagree and submit that the "subject matter of the claim need not be described literally (i.e., using the same terms or *in haec verba*) in order for the disclosure to satisfy the description requirement." (MPEP §2163.02) (emphasis in original).

Applicants respectfully submit that "a computer readable storage medium" is supported by the original disclosure under 35 U.S.C. §112, first paragraph. The specification discloses the following:

> "Computer useable medium <u>comprising a computer program code that is configured to cause a processor to execute one or more functions to perform a method</u> for retrieving medical images from various sources and in different formats, to enable the creation of teaching files and research datasets, for the building of a personal medical image library, the method comprising: (a) retrieving a plurality of medical images from various sources; (b) storing the plurality of medical images in a database; (c) generating a database record for the teaching files and research datasets; (d) generating the teaching files and research datasets file ; (e) saving the teaching files and research datasets into the database; and generating at least one index of the teaching files and research datasets."

(specification, p. 13, line 31- p. 14, line 5)(emphasis added).

Applicants respectfully submit that one of ordinary skill in the art will understand that a "computer useable medium comprising a computer program code that is configured to cause a processor to execute one or more functions..." is a computer readable storage medium. A computer readable storage medium is inherently disclosed by definition of the program code contained in the medium that is configured to cause a processor to execute one or more functions. One of ordinary skill in the art understands that the medium containing the program code configured to cause a processor to execute one or more functions is a computer readable storage medium.

Therefore, applicants respectfully request the Examiner to withdraw the objection to the specification.

Claims 1-37 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 7,374,077 to Shimura ("Shimura") and further in view of U.S. Patent No. 7,080,098 to Smirniotopoulos ("Smirniotopoulos").

Applicants do not admit that Shimura is prior art and reserve the right to swear behind Shimura at a later date. Applicants do not admit that Smirniotopoulos is prior art and reserve the right to swear behind Smirniotopoulos at a later date.

Amended claim 1 reads as follows:

> A method for retrieving medical images from various sources and in different formats, to enable the creation of teaching files and research datasets, for the building of a personal medical image library, the method comprising:
> (a) directly retrieving a plurality of medical images from various sources;
> (b) storing the plurality of medical images in a database;
> (c) generating a database record for the teaching files and research datasets;
> (d) generating the teaching files and research datasets using at least one medical image of the plurality of medical images and additional information input by a user, the teaching files and research datasets being compliant with at least one predetermined schema;
> (e) saving the teaching files and research datasets into the database;
> (f) generating at least one index of the teaching files and research datasets; and

> (g) automatically anonymizing patient identification data when the at least one medical image is retrieved from the various sources, wherein the patient identification data comprises patient sensitive information that is not revealed publicly, wherein the automatic anonymizing of patient identification data includes replacing each item of the patient identification data with an anonymization code.

(emphasis added)

Amended claim 1 now includes substantially all limitations of original claim 7. Applicants have canceled the original claim 7.

The support under 35 U.S.C. §112, first paragraph for amended claim 1 is found in the specification, for example, at page 11, lines 1-8. The anonymization process involving automatically anonymizing patient identification data when the at least one medical image is retrieved from the various sources, wherein the patient identification data comprises patient sensitive information that is not revealed publicly, wherein the automatic anonymizing of patient identification data includes replacing each item of the patient identification data with an anonymization code, as recited in amended claim 1, gives the user the opportunity to further request the information about the patient identification data using the anonymization code, since in accordance with various embodiments, the correspondence relationship- a mapping table- between the-sensitive information and the anonymized code is stored in the database.

With respect to the rejections under 35 U.S.C. §103, the Examiner acknowledged that "Shimura does not explicitly disclose the following: (g) automatically anonymizing patient identification data when the at least one medical image is retrieved from the various sources, wherein the patient identification data comprises patient sensitive information that is not revealed publicly."(Office Action, p. 5).

Shimura discloses a similar image search system which includes an image database storing a plurality of images. Search image data representing the whole or a part of an image to which a feature is to be searched for, is input into the system. A searching means of the system searches the database for similar images stored in the database. If image data similar to the input image data to be searched for are found in the database, these image data are output to a user on a display means.

Accordingly, Shimura fails to disclose automatically anonymizing patient identification data when the at least one medical image is retrieved from the various sources, wherein the patient identification data comprises patient sensitive information that is not revealed publicly, wherein the automatic anonymizing of patient identification data includes replacing each item of the patient identification data with an anonymization code, as recited in amended claim 1.

The Examiner alleges that "Smirniotopolous teaches: automatically anonymizing patient identification data when the at least one medical image is retrieved from the various sources... (col. 3, lines 37-67 through col. 4, lines 1-7), wherein the patient identification data comprises patient sensitive information that is not revealed publicly...(col. 3, lines 55-61)." (Office Action, p. 5). With respect to original claim 7, the Examiner alleges that "Smirniotopolous_teaches:...the automatic anonymizing of patient identification data process includes replacing of each item of the sensitive information with an anonymization code (col. 4, lines 41-57)."(Office Action, pages 6-7).

Applicants respectfully disagree with this interpretation for at least the following reasons.

The portions in Smirniotopolous (col. 3, line 30-col. 4, line 7) referred by the Examiner disclose the following:

> Turning now to FIG. 2, an overview of the multimedia medical database's functionality is provided from the user's perspective. In the preferred system implementation, the first user step will be an access logon (step 201). This typically includes a user presentation of their system name and a password, although additional levels of security and access control schemes may be used where more sensitive information is being stored. Thus, multiple levels of privileges may be supported, such as for an author of a file, a reviewer, an editor, a guest, and a system administrator. The level of privileges may also vary based upon the state of the file and the particular information being manipulated. For example, where a user with author privileges has the full ability to create a new file, certain fields (such as factoid categories) in the file may still be locked

> against subsequent changes by the author after the file has been approved by an editor. Similarly, an author may not have privileges to edit modifications like reviewer comments. Moreover, multi-level access control, using role-based or other schemes, may be advantageously employed. Which approach to adopt is a matter of design choice that one skilled in the art would understand how to implement. When using a multi-level system, e.g., the same registered user could be qualified for all five types of privileges, with the particular privilege being determined based upon the file or information within the file that is being accessed. Thus, even though a person acted as both author and editor of a given file, it is possible that after approval he could be restricted to visitor status with respect to certain file access, and may lack even these privileges with respect to portions of the file (e.g., sensitive patient information, where his role has changed vis-a-vis the patient's care). Such versatility can be very handy when dealing with sensitive information, but this must be balanced against the complexity of administering multilevel access.
>
> Once a user is registered with the system, he or she proceeds to select the particular process that they want to use (step 205). For many users, the most common processes will be browsing or searching through case files (step 250), or adding new cases to the database (step 210). In addition to these two processes, some of the users will be accessing the editor routine (step 220), working with teaching files (step 240), or other specialized review processes such as the consultation process of step 230. The system may also be designed to mask those processes, or options within a given process, for which a user does not have sufficient privileges.

(Smirniotopolous, col. 3, line 30-col. 4, line 7)(emphasis added)

Thus, illustratively, the above passages merely disclose the protection of stored data by means of an access control scheme, in other words, by using a scheme in which no information (except for at best a denial of access information) is output to the user. Thus, there is no anonymization process carried out in accordance with Smirniotopoulos. To the contrary, the data records are stored in plain text, but the access to the records may be denied for a user in accordance with Smirniotopoulos. Therefore, Smirniotopoulos teaches away from carrying out an anonymization process, and even more from replacing of each item of the patient identification data with an anonymization code, as claimed in amended independent claim 1.

The passage "The system may also be designed to mask those processes, or options within a given process, for which a user does not have sufficient privileges" in Smirniotopoulos merely discloses that the respective access selection is not shown to the user, i.e. it is invisible to the user for selection; however, this again fails to disclose to carry out an anonymization process, in particular an anonymization process including replacing of each item of the patient identification data with an anonymization code, as claimed in amended independent claim 1.

Further, the portions in Smirniotopoulos (col. 4, lines 41-57) cited by the Examiner disclose the following:

> A variety of other data-capture tools_may also be presented. If the user is a radiologist, a pull-down menu may be used to help them rapidly select appropriate ACR radiology codes. By hierarchically linking the data available for the pull-down menus, a user can rapidly progress from general systems down to the unique name or code identifying the particular condition or disease. Other well-known codes, such as the ICD codes, may be used as appropriate. A user community may also find it convenient to implement a more generic coding system, such as the MedPix codes block that is illustrated in connection with FIG. 3. In developing such coding schemes, it is useful to allow certain users to have privileges to add new entries to the pull-down lists, such as the Add New Category box 305 for MedPix codes 303. Thus, through interaction with the broader user community, a more tailored hierarchical coding structure can be rapidly developed for that community.

(col. 4, lines 41-57)(emphasis added)

As set forth above, Smirniotopoulos discloses the selecting the appropriate codes. In particular, Smirniotopoulos discloses that by linking the data available for the pull-down menus, a user can progress down to the unique name or code. In contrast, amended claim 1 refers to replacing each item of the patient identification data with an anonymization code. Smirniotopoulos does not disclose automatically anonymizing patient identification data when the at least one medical image is retrieved from the various sources, wherein the patient identification data comprises patient sensitive information that is not revealed publicly, wherein the automatic anonymizing of patient identification data includes replacing each item of the patient identification data with an anonymization code, as recited in amended claim 1.

It is respectfully submitted that Shimura does not teach or suggest a combination with Smirniotopoulos, and Smirniotopoulos does not teach or suggest a combination with Shimura. It would be impermissible hindsight, based on applicants' own disclosure to combine Shimura and Smirniotopoulos.

Furthermore, even if the medical multimedia database system of Smirniotopoulos were incorporated into the image search system of Shimura, such a combination would still lack automatically anonymizing patient identification data when the at least one medical image is retrieved from the various sources, wherein the patient identification data comprises patient sensitive information that is not revealed publicly, wherein the automatic anonymizing of patient identification data includes replacing each item of the patient identification data with an anonymization code, as recited in amended claim 1.

Therefore, applicants respectfully submit that claim 1, as amended, is not obvious under 35 U.S.C. 103(a) over Shimura in view of Smirniotopoulos.

Given that independend amended claims 21 and 37 contain limitations that are similar to those limitations set forth above, applicants respectfully submit that claims 21 and 37, as amended, are not obvious under 35 U.S.C. 103(a) over Shimura in view of Smirniotopoulos.

Given that claims 2-20, and 22-36 depend from amended claims 1 or 21 respectively, and add additional limitations, applicants respectfully submit that claims 2-20, and 22-36 are not obvious under 35 U.S.C. §103(a) over Shimura in view of Smirniotopoulos.

Claims 24-28 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Shimura and further in view of U.S. Publication No. 2003/0013951 to Stefanescu ("Stefanescu").

Applicants do not admit that Stefanescu is prior art and reserve the right to swear behind Stefanescu at a later date.

As set forth above, even if the medical multimedia database system of Smirniotopoulos were incorporated into the image search system of Shimura, such a combination would still lack automatically anonymizing patient identification data when the at least one medical image is retrieved from the various sources, wherein the patient identification data comprises patient sensitive information that is not revealed publicly, wherein the automatic anonymizing of patient identification data includes replacing each item of the patient identification data with an anonymization code, as recited in amended claim 1.

Stefanescu, in contrast, discloses organizing and searching database of medical images. Stefanescu fails to disclose or suggest an MIRC server configured to provide an MIRC file storage service for the database and for a user's machine automatically anonymizing patient identification data based upon the at least one medical image retrieved from the various sources, wherein the patient identification data comprises patient sensitive information that is not revealed publicly, wherein the automatic anonymizing of patient identification data includes replacing each item of the patient identification data with an anonymization code, as recited in amended claim 1.

It is respectfully submitted that none of the references cited by the Examiner teach or suggest a combination with each other. It would be impermissible hindsight, based on applicants' own disclosure to combine Stefanescu, Shimura and Smirniotopoulos.

Furthermore, even if the database organization and searching of Stefanescu and medical multimedia database system of Smirniotopoulos were incorporated into the image search system of Shimura, such a combination would still lack automatically anonymizing patient identification data based upon the at least one medical image retrieved from the various sources, wherein the patient identification data comprises patient sensitive information that is not revealed publicly, wherein the automatic anonymizing of patient identification data includes replacing each item of the patient identification data with an anonymization code, as recited in amended claim 21.

Given that claims 24-28 depend from amended claim 21, and add additional limitations, applicants respectfully submit that claims 24-28 are not obvious under 35 U.S.C. §103(a) over Shimura in view of Smirniotopoulos.

It is respectfully submitted that in view of the amendments and arguments set forth herein, the applicable rejections and objections have been overcome. If the Examiner believes a telephone conference would assist in the prosecution of the present application, the Examiner is invited to call the undersigned.

If there are any additional charges, please charge Deposit Account No. 022666 for any fee deficiency that may be due.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: June 7, 2010

/TatianaRossin/
Tatiana Rossin
Reg. No.: 56,833

1279 Oakmead Parkway
Sunnyvale, California 94085-4040
(408) 720-8300

Customer No. 087901